MSIX
Migrant Student Information Exchange

Information Security

WHAT IS PERSONALLY IDENTIFIABLE INFORMATION?

Personally Identifiable Information (PII) is information that, alone or in combination, **is linked or linkable to a specific student** that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty.

PROTECTING PII

- MSIX **contains real, sensitive data** that could cause great harm if it were stolen or intercepted. Student data in MSIX could be used maliciously for identity theft, leading to financial and legal issues for those affected.
- Users can **encrypt** their files using "zipping" applications such as WinZip. However, if you do not have WinZip or a similar program, many Microsoft Office products offer the ability to password protect files.

If there is a PII incident, users should contact the MSIX Help Desk immediately at 1-866-878-9525

CONTACTING THE HELP DESK

ENHANCEMENT REQUESTS

- Users can **submit their ideas** to improve MSIX directly to the Help Desk.
- If the enhancement request is approved it will be deployed in a future release.
- To **submit** an Enhancement Request call the Help Desk at **1-866-878-9525** or email your idea to **MSIXSupport@Deloitte.com.**

SENDING SCREENSHOTS

- The Help Desk will only ask for screenshots or any other information with PII when there is no other approach available.
- Users will be instructed to **obscure or encrypt** the PII.
- Unencrypted PII sent to the Help Desk will be **permanently deleted** from all mailboxes.

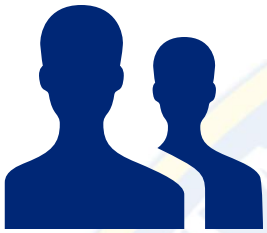
WHY IS FILE ENCRYPTION IMPORTANT?

- Encryption makes it more **difficult for unauthorized persons** to access student data.
- When communicating electronically with colleagues inside and out of your State MEP, it is critical to **encrypt all files that contain student data,** e.g., emailing a student's Consolidated Record.
- Once you have encrypted your file, **send it in a email separate from the password**. This is an extra security measure in case one of your emails is intercepted.
- For **instructions on how to encrypt your file**, contact the Help Desk.

MSIX
Migrant Student Information Exchange

Information Security

SOCIAL ENGINEERING



- Social Engineering is the **manipulation of people into performing actions or divulging confidential information**. In many cases it is easier for hackers to socially engineer a password then use their technical skills to crack it.
- One form of social engineering is Pretexting, or **the use of information to impersonate a person of authority**, e.g., stating your MSIX username to establish legitimacy over the phone.
- The Help Desk will **never ask you for your password** and you should never give it out over the phone, email, or in person.
- If you receive a suspicious email or phone call you should **contact the Help Desk immediately.**

FEDERAL SECURITY LAWS AND MSIX

- The Family Educational Rights and Privacy Act (FERPA) is a Federal law that **protects the privacy of student education records**.
- FERPA permits a State Education Agency (SEA) to transfer, without parental consent, **minimum data elements (First Name, Birth Country, Course Title, etc.) of the migratory student record to MSIX**, and to use MSIX to transfer, without parental consent, the minimum data elements of the migratory student to another SEA or Local Education Agency (LEA).
- The Federal Information Security Management Act (FISMA) requires each federal agency to **develop, document, and implement information security** to reduce risks to an acceptable level.

PHYSICAL SECURITY

- Do not leave student records **or PII in public view on your desk or printer**; it only takes one visitor walking through the office to create a PII incident.
- **Lock your computer or tablet** with a password when leaving it unattended. If you use a laptop, physically lock it to your desk with **a cable cord.**
- Properly **secure sensitive information** such as printed student records.
- Do not leave your username or password in a public place, e.g., **written on a sticky note attached to your monitor.**